

I. General Remarks Concerning This Response

Claims 1-21 are currently pending in the present application. No claims have been amended, added, or canceled. Reconsideration of the claims is requested.

5

II. Summary of Telephonic Interview

Applicant thanks Examiner Burgess for the telephonic interview of 08/28/2003. During this interview, Applicant summarized the important differences between the applied prior art and the present invention; this response contains a formal presentation of the arguments that were briefly presented during the interview. At the time of the interview, the examiner did not agree to accept Applicant's interpretation of the prior art and reserved judgment on the merits of Applicant's arguments until the arguments were presented within this formal response.

III. Summary of Present Invention

An enterprise computing environment, such as a corporate web portal, includes an intermediary server, a sign-on service, and one or more backend enterprise systems managed by resource managers. Before or after user primary logon, which establishes a user primary account identity, the intermediary server uses its own identity to authenticate to the sign-on service its right to retrieve user secondary account identities with respect to the backend enterprise systems. Retrieved secondary account identities are then used by the intermediary server to perform user secondary logons to respective resource managers in the environment. The intermediary server also manages the passing of resource requests and associated replies between the user and the resource managers.

IV. 35 U.S.C. § 102(b)-Anticipation-Hu

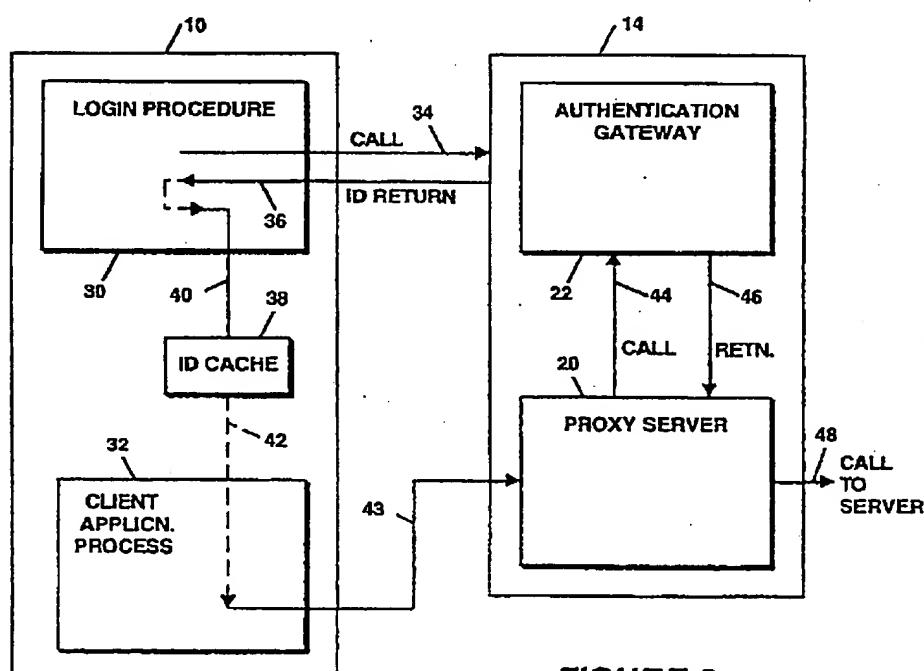
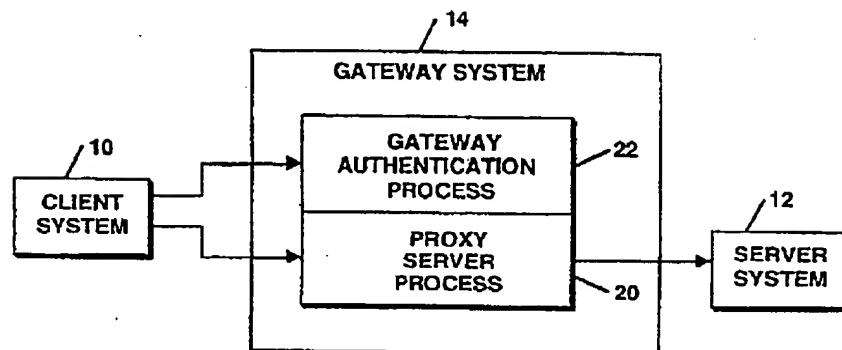
The Office action has rejected independent claims 1-6, 8-14, 16, 17, and 19-21 under 35 U.S.C. § 102(b) as anticipated by Hu, "Method and apparatus for authenticating a client to a server in computer systems which support different security mechanisms", U.S. Patent No. 5,586,260, filed 02/12/1993, issued 12/17/1996. This rejection is traversed.

All of the pending independent claims have been rejected over Hu. Each of these independent claims has one or more common elements against which the rejection applies certain portions of Hu. However, Applicant asserts that there is at least one element of each independent claim that is not shown in Hu, thereby causing these anticipation rejections to be deficient. However, prior to discussing these rejections in more detail, Applicant makes the following preliminary comparison of Hu and the present invention.

The abstract of Hu states in its entirety:

A method and corresponding apparatus for authenticating a client for a server when the client and server have different security mechanisms. An intermediary system known as an authentication gateway provides for authentication of the client using the client security mechanism, and impersonation of the client in a call to a server that the client wishes to access. The client logs in to the authentication gateway and provides a user name and password. Then the authentication gateway obtains and saves security credentials for the client, returning an access key to the client. When the client wishes to call the server, the client calls the authentication gateway acting as a proxy server, and passes the access key, which is then used to retrieve the security credentials and to impersonate the client in a call to the server. Any output arguments resulting from the call to the server are returned to the client through the authentication gateway.

These steps are shown within FIG. 2 and FIG. 3 of Hu:



Hu explains its Figure 2 and Figure 3 at lines 5 through 58 in column 4 as follows:

5 FIG. 2 shows the gateway computer system 14 as including a proxy server process 20 and an authentication gateway process 22. As will be further explained, the authentication gateway process 22 authenticates the client within the client security domain 18. When the client system 10 makes a request to use the server 12, 10 the request is processed by the proxy server 20, which obtains the client credentials from the gateway authentication process 22, and then makes a call to the real server 12, effectively impersonating the client 10. If the service requested of the server 12 requires that information be passed back to the client from the server, this information is passed through the proxy server 20 acting as an intermediary.

15 FIG. 3 takes the explanation of the authentication gateway scheme one step further, and shows diagrammatically the sequence 20 of steps followed by each of the systems in handling access to the server 12 by a client system 10 not conforming with the security mechanism of the server. The client system 10 includes a log-in 25 procedure 30, and a client application process 32 from which a server request will emanate. The log-in procedure 30 is executed, as its name implies, only infrequently, such as once a day. Part of the log-in procedure is a call to the authentication gateway 22 to permit authentication within the client security domain. This 30 call, indicated by line 34 carries as parameters the identity of the client and any necessary password or security code needed to satisfy the security requirements of the client security domain. The authentication gateway 22 performs the operations necessary to verify the authenticity of the client 10. The authentication 35 gateway 22 acquires authentication credentials for the client and saves them for later use. The authentication gateway 22 then returns to the log-in procedure 30, over line 36, an identifier that confirms authentication of the client. The log-in procedure 30 stores the returned identifier in an id. cache 38. This completes the first phase of operation of the gateway, which has 40 authenticated the client within the client's security domain and has stored a confirming identifier in the cache 38, over line 40 for later use by the client.

40 Subsequently, when the client application process 32 wishes to make a call to the server, the contents of the id. cache are retrieved, as indicated by the broken line 42, and the client makes a call to the proxy server process 20, as indicated by line 42, passing as an argument of the call the identifier obtained 45 from the cache 38. Then, using the identifier, the proxy server 20 calls the authentication gateway 22, as indicated by line 44, and acquires, over line 46, the credentials of the client that were saved by the authentication gateway during the log-in procedure. At this point the proxy server has all the information 50 it needs to make a call to the real server 12, as indicated by line 48. Information generated as a result of the call to the server 12 is passed back to the client application process 32, through lines 48 and 43.

As stated in column 5, lines 63-65: "The log-in procedure prompts the user for a user name and a password based on the server security domain." Thus, in the system disclosed in Hu,
5 a user has one user identity for each security domain that the user accesses. The credentials that result from the login procedure are cached by the authentication gateway process 22 for later use by the proxy server process 20; these two entities subsequently interact when the proxy server process 10 calls the authentication gateway process to retrieve the previously cached credential for a particular security domain. Hence, the system of Hu is useful because a user performs multiple login procedures for the multiple server security domains that are accessed, and the cached credentials may be 15 re-used without the user having to perform the login procedure again.

However, the system of Hu does not disclose a plurality of user identities that are derived from a single user identity and then used by a single-sign-on service, such as a 20 primary user identity and a set of secondary user identities as disclosed and claimed in the present patent application. As explained in more detail further below, Applicant asserts that the rejection has misinterpreted the manner in which the system of Hu employs multiple user identities and improperly 25 states that Hu discloses the employment of multiple user identities as taught by the present invention.

With reference now to independent claim 1, Applicant asserts that Hu does not disclose all of the elements of claim 1. The rejection states in its entirety:

30 As per claim 1, Hu discloses a method of enabling a client terminal user to access target resources managed by a set of resource managers within an enterprise computing environment, comprising:

authenticating the user to establish a user primary identity (column 1, lines 52-55, column 2, lines 3-5, 30-35, 42-45, column 4, lines 23-28);

5 mapping the user primary identity to a set of user secondary identities (column 2, lines 1-17, 20-25, 42-47, column 4, lines 44-55, column 5, lines 30-35, 60-67, column 6, lines 1-11, 17-30);

10 authenticating the user to the resource managers using the set of secondary identities (column 2, lines 1-17, 20-25, 42-47, column 4, lines 44-55, column 5, lines 30-35, 60-67, column 6, lines 1-11, 17-30);

15 following authentication using the set of user secondary identities, forwarding resource requests to the resource managers (column 3, lines 63-65, column 4, lines 53-55, column 6, lines 31-35);

returning replies received from the resource managers back to the user (column 4, lines 14-17, 55-58, column 6, lines 35-39).

20 As should be apparent from a cursory reading of the rejection, the rejection has taken multiple shortcuts in terms of form and logic that make it difficult for one to understand the anticipation argument that is supposedly presented by the rejection. For example, it is difficult to understand why the same portions of Hu are cited as disclosing different elements within the claim. Additionally, it is difficult to understand why multiple portions of Hu are cited for disclosing one element within the claim. Moreover, some of the cited portions of Hu contain many different kinds of processing steps, and it is difficult to understand why the anticipation rejection does not attempt to relate individual steps within Hu to the individual steps in the method of claim 1. Thus, Applicant must attempt to construct a logical argument from the cited portions without any additional statements within the rejection.

30 Applicant asserts that Hu does not disclose "a user primary identity" nor "a set of user secondary identities". Hence, it is not possible for Hu to disclose the second

element of claim 1, "mapping the user primary identity to a set of user secondary identities".

Even though Hu does not disclose a user primary identity, one could argue that it does disclose a user identity, and
5 then one could proceed to consider this user identity as a user primary identity. From that point, one could argue that the first element of claim 1, "authenticating the user to establish a user primary identity", is disclosed by the login procedure 30 that is shown in Figure 3 of Hu. As noted above, 10 the user provides a user name (user identity) during the login procedure based on the security domain. This authentication procedure results in a single cached identifier that relates to the cached credentials for a security domain. This cached identifier is subsequently provided to the proxy server 20, 15 which then provides the identifier to the authentication gateway 22.

The authentication gateway then uses the identifier to retrieve the credentials that were previously saved by the authentication gateway during a login procedure; the 20 identifier associates the credentials for a security domain with the user identity that was provided during the login procedure. In this manner, the authentication gateway maps a single user identity to the credentials for the security domain that was used in the login procedure. However, Hu does 25 not disclose "mapping the user primary identity to a set of user secondary identities", as claimed in claim 1.

Taking a different approach, one could argue that Hu does disclose a set of user identities, each of which is associated with a security domain; the user must provide a user name and 30 a password for each security domain into which the user performs a login procedure. One could proceed to argue that these user identities are a set of user secondary identities.

From that point, one could argue that the third element of claim 1, "authenticating the user to the resource managers using the set of user secondary identities", is disclosed by multiple repetitions of the login procedure 30 that is shown 5 in Figure 3 of Hu. However, one would not be able to argue that Hu discloses a user primary identity nor, more importantly, "authenticating the user to establish a user primary identity", as stated in the first element of claim 1. Each of the user identities in Hu should be considered as 10 having similar characteristics, and no user identity is distinguished as being a user primary identity. Moreover, Hu still does not disclose "mapping the user primary identity to a set of user secondary identities", as stated in the second element of claim 1.

15 Hence, Hu does not disclose at least one element of claim 1 as is required for a proper anticipation rejection. As stated at MPEP § 2131: "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). 20 25 Hence, the rejection of claim 1 is improper, and Applicant requests that the rejection be withdrawn.

Dependent claims 2-6, 8, and 9 are patentable for the same reasons as independent claim 1 based on their incorporation of claim 1. Dependent claim 7 is addressed by 30 an obviousness-type rejection. Dependent claim 8 merely states that the client uses the Internet, while dependent claim 9 merely states that an authentication service that is

associated with a resource manager performs an authentication operation.

However, dependent claims 2-6 incorporate some form of processing on a set of secondary user identities, so these features also are not disclosed in Hu, thereby providing additional reasons for the patentability of claims 2-6.

Dependent claim 2 states that "the user primary identity is mapped to the set of user secondary identities by a sign-on service", while claim 3 includes an additional element of "authenticating a trusted server to the sign-on service" prior to the mapping step. Claim 4 states that "the trusted server is authenticated to the sign-on server" before the step of authenticating the user primary identity, and claim 5 states that "the trusted server is authenticated to the sign-on service" after the step of authenticating the user primary identity. Claim 6 states that "the user is authenticated to establish the user primary identity using an authentication service associated with the trusted server". Hu does not disclose a differentiation and a mapping between a user primary identity and a set of user secondary identities, as discussed above with respect to independent claim 1, and Hu does not disclose the additional elements concerning a particular order in the steps of using a trusted server, as recited in the dependent claims of independent claim 1, notwithstanding the recitations within the rejection of the dependent claims to the the same sections of Hu that were cited against claim 1.

Independent claim 10 includes the elements of "using the user primary identity, accessing the sign-on service to retrieve a set of stored user authentication information, wherein the stored user authentication information comprises a set of user secondary identities" and "performing a sign-on to

the set of resource managers using the retrieved set of user secondary identities". Hence, for reasons similar to those that were argued above with respect to independent claim 1, independent claim 10 includes features that are not disclosed 5 in Hu, and claim 10 is also patentable because Hu does not disclose at least one element of claim 10 as is required for a proper anticipation rejection.

With respect to independent claim 11, this claim also recites various elements concerning a user primary identity 10 and a set of user secondary identities. In fact, claim 11 recites additional elements that would require additional disclosure in Hu, yet Hu does not disclose these additional features, notwithstanding the recitations within the rejection of independent claim 11 to the the same sections of Hu that 15 were cited against claim 1. For example, claim 11 recites the following element: "having the intermediary server pass the user's primary identity to the sign-on service and, in response, obtaining a set of user secondary identities that may be used in enabling the intermediary server to represent 20 the client terminal user to the resource managers". Hence, for reasons similar to those that were argued above with respect to independent claim 1, independent claim 11 has features that are not disclosed in Hu, and claim 11 is also 25 patentable because Hu does not disclose at least one element of claim 11 as is required for a proper anticipation rejection.

Independent claim 12 is similar to independent claim 1, but claim 12 is a type of system claim whereas claim 1 is a method claim. For example, claim 12 includes the elements of 30 "means for authenticating a user to establish a user primary account associated with a user primary identity" and "means for cooperating with the sign-on service to map the user

primary account to a set of user secondary accounts associated with a set of user secondary identities". Hence, for reasons similar to those that were argued above with respect to independent claim 1, independent claim 12 includes features 5 that are not disclosed in Hu, and claim 12 is also patentable because Hu does not disclose at least one element of claim 12 as is required for a proper anticipation rejection.

Dependent claim 13 merely states that the server returns replies for resource requests back to the user, but dependent 10 claim 13 is patentable for the same reasons as independent claim 12 based on its incorporation of claim 12.

Independent claim 14 is similar to independent claim 1, but claim 14 is a type of server claim whereas claim 1 is a method claim. For example, amended claim 14 includes the 15 elements of "means for authenticating a user to establish a user primary account associated with a user primary identity" and "means for logging onto the set of resource managers using a set of user secondary accounts returned from the sign-on service, wherein the set of user secondary accounts is associated with a set of user secondary identities". Hence, 20 for reasons similar to those that were argued above with respect to independent claim 1, independent claim 14 includes features that are not disclosed in Hu, and claim 14 is also patentable because Hu does not disclose at least one element 25 of claim 14 as is required for a proper anticipation rejection. Dependent claim 15, which depends from claim 14, is addressed in a obviousness-type rejection.

Independent claim 16 is similar to independent claim 1, but claim 16 is a type of system claim whereas claim 1 is a method claim. For example, claim 16 includes the elements of 30 "means for authenticating users to establish user primary accounts associated with user primary identities" and "means

for logging a given user onto the set of resource managers using a set of user secondary accounts for the given user retrieved from the sign on service, wherein a set of user secondary accounts for a given user is associated with a set 5 of user secondary identities for a given user". Hence, for reasons similar to those that were argued above with respect to independent claim 1, independent claim 16 includes features that are not disclosed in Hu, and claim 16 is also patentable because Hu does not disclose at least one element of claim 16 10 as is required for a proper anticipation rejection.

Dependent claims 17-20 are patentable for the same reasons as independent claim 16 based on their incorporation of claim 16. Dependent claim 18, which depends from claim 16, is addressed in a obviousness-type rejection. Dependent 15 claims 17, 19, and 20 merely recite a plurality of servers or resource managers.

Independent claim 21 is similar to claim 14; claim 21 is directed to a computer program product, whereas claim 14 is directed to a server. Hence, for reasons similar to those 20 that were argued above with respect to independent claims 1 and 14, independent claim 21 includes features that are not disclosed in Hu, and claim 21 is also patentable because Hu does not disclose at least one element of claim 21 as is required for a proper anticipation rejection.

25

V. 35 U.S.C. § 103(a)-Obviousness-Grantges in view of Brendel et al.

The Office action has rejected claims 7, 15, and 18 under 35 U.S.C. § 103(a) as unpatentable over Hu in view of Brendel 30 et al., "World-Wide-Web Server with Delayed Resource-Binding for Resource-Based Load Balancing on A Distributed Resource

Multi-Node Network, filed 08/05/1996, issued 06/30/1998. This rejection is respectfully traversed.

With respect to dependent claims 7, 15, and 18, the rejection properly states that Brendel et al. discloses a load-balancing mechanism as recited in claims 7, 15, and 18. However, claims 7, 15, and 18 depend from claims 1, 14, and 16, respectively, and as argued above, Hu fails to disclose the features of these independent claims. Moreover, Brendel et al. also fails to disclose the features of these independent claims. Hence, a combination of the teaching of Brendel et al. with Hu cannot support a rejection of dependent claims 7, 15, and 18 because at least one feature of the independent claims has not been disclosed in the prior art. Applicant respectfully submits that more than one claimed feature is not shown in the prior art references nor can the teachings of the references be combined to disclose the present invention. Hence, the rejection of claims 7, 15, and 18 does not establish a *prima facie* case of obviousness based on the prior art. Therefore, the rejection of claims 7, 15, and 18 under 35 U.S.C. § 103(a) has been shown to be insupportable, and these claims are patentable over the applied references. Applicant requests that the rejection be withdrawn.

25 VI. Conclusion

It is respectfully urged that the present patent application is patentable, and Applicant kindly requests a Notice of Allowance.

For any other outstanding matters or issues, the examiner is urged to call or fax the below-listed telephone numbers to expedite the prosecution and examination of this application.

5 DATE: October 6, 2003

Respectfully submitted,


Joseph R. Burwell

Reg. No. 44,468

ATTORNEY FOR APPLICANT

10

15

Law Office of Joseph R. Burwell
P.O. Box 28022
Austin, Texas 78755
Voice: 866-728-3688 (866-PATENT8)
Fax: 866-728-3680 (866-PATENT0)
Email: joe@burwell.biz